In the Claims

1. (Currently Amended) A method ~~for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network~~, comprising:

receiving a request for connection from an initiator, over ~~the public~~ a public network;

a routing device requesting an acknowledgment from the initiator of the request, wherein the routing device interconnects a private network to the public network;

determining whether the acknowledgment has been received within a specific predetermined amount of time;

adding an IP address of the initiator to a cache of IP addresses if the acknowledgement is not received; and

denying the request if the acknowledgment is not received within the specific predetermined amount of time.

2. (Original) The method of Claim 1, wherein the public network is the Internet.

3. (Original) The method of Claim 2, wherein the routing device is a firewall providing access to the Internet.

4. (Original) The method of Claim 1, further comprising processing the request if the acknowledgement is received.

5. (Canceled)

6. (Currently Amended) The method of ~~Claim 5~~ Claim 1, further comprising denying access through the routing device to any IP address on the cache of IP addresses.

7. (Original) The method of Claim 1, further comprising storing information about the initiator on a system log for analysis by the system administrator.

8. (Original) The method of Claim 1, further comprising storing information about the request for connection on a system log for analysis by the system administrator.

9. (Original) The method of Claim 1, further comprising determining if a prior request for an acknowledgement has been sent to an IP address associated with the initiator and been unacknowledged within a predetermined amount of time, if the acknowledgement is not received.

10. (Original) The method of Claim 1, further comprising using diagnostic tools to determine additional information about a source of the request for connection.

11. (Original) The method of Claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using trace root diagnostic tools to determine information about the source of the request for connection.

12. (Original) The method of Claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using ping diagnostic tools to determine information about the source of the request for connection.

13. (Original) The method of Claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using NS lookup diagnostic tools to determine information about the source of the request for connection.

14. (Original) The method of Claim 10, further comprising forwarding the additional information to a system administrator via electronic mail.

15. (Currently Amended) A method ~~for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network~~, comprising:

receiving an incoming data packet from ~~the public~~ a public network;

a routing device comparing a source address of the data packet against known internal addresses of [[the]] a private network, wherein the routing device interconnects the private network to the public network;

determining if the source address matches a known internal address; and

if there is a match:

dropping the data packet;

analyzing a header of the data packet;

determining information regarding a history of the packet;

determining a real source of the data packet using the information regarding the history of the packet;

adding an IP address of the data packet to a cache of IP addresses; and

refusing to process any additional data packets received from the real source of the data packet.

16. (Original) The method of Claim 15, further comprising storing data about the data packet on a system log, for use and analysis by a system administrator.

17. (Original) The method of Claim 15, wherein the public network is the Internet.

18. (Original) The method of Claim 17, wherein the routing device is a firewall providing access to the Internet.

19. (Original) The method of Claim 15, further comprising forwarding the data packet to the private network if there is not a match.

20. (Canceled)

21. (Currently Amended) The method of ~~Claim 20~~ Claim 15, further comprising denying access through the routing device to any IP address on the cache of IP addresses.

22. (Original) The method of Claim 15, further comprising using diagnostic tools to determine additional information about a source of the data packet.

23. (Original) The method of Claim 22, wherein using diagnostic tools to determine additional information about a source of the data packet comprises using trace root diagnostic tools to determine additional information about the source of the data packet.

24. (Original) The method of Claim 22, wherein using diagnostic tools to determine additional information about a source of the data packet comprises using ping diagnostic tools to determine additional information about the source of the data packet.

25. (Original) The method of Claim 22, wherein using diagnostic tools to determine additional information about a source of the data packet comprises using NS lookup diagnostic tools to determine additional information about the source of the data packet.

26. (Original) The method of Claim 22, further comprising forwarding the additional information to a system administrator via electronic mail.

27. (Currently Amended) A method ~~for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network~~, comprising:

receiving a request for connection from an initiator, over ~~the public~~ a public network;

a routing device requesting an acknowledgment from the initiator of the request, wherein the routing device interconnects a private network to the public network;

determining whether the acknowledgment has been received within a specified predetermined amount of time;

denying the request if the acknowledgment is not received within the specified predetermined amount of time;

comparing a source address of the request for connection with known internal addresses of the private network;

determining if the source address matches a known internal address;

adding an IP address of the data packet to a cache of IP addresses if there is a match; and

refusing to process the request for connection if there is a match.

28. (Currently Amended) A system ~~for blocking an attack on a private network~~, comprising:

a routing device being operable to interconnect a private network to a public network, the routing device being further operable to:

receive a request for connection from an initiator, over the public network;

request an acknowledgment from the initiator of the request;

determine whether the acknowledgment has been received within a specified predetermined amount of time;

add an IP address of the initiator to a cache of IP addresses if the acknowledgement is not received; and

deny the request if the acknowledgment is not received within the specified predetermined amount of time.

29. (Currently Amended) A system ~~for blocking an attack on a private network~~, comprising:

a routing device being operable to interconnect ~~the public~~ a public network and a public network, the routing device being further operable to:

receive an incoming data packet from the public network;

compare a source address of the data packet against known internal addresses of the private network;

determine if the source address matches a known internal address; and

if there is a match:

drop the data packet;

analyze a header of the data packet;

determine information regarding a history of the packet;

determine a real source of the data packet using the information regarding the history of the packet;

adding an IP address of the data packet to a cache of IP addresses; and

refuse to process any additional data packets received from the real source of the data packet.

30. (Currently Amended) A system ~~for blocking an attack on a private network~~, comprising:

means for interconnecting a private network to a public network;

means for receiving a request for connection from an initiator, over the public network;

means for requesting an acknowledgment from the initiator of the request;

means for determining whether the acknowledgment has been received within a specified predetermined amount of time;

means for adding an IP address of the initiator to a cache of IP addresses if the acknowledgement is not received; and

means for denying the request if the acknowledgment is not received within the specified predetermined amount of time.

31. (Currently Amended) A system ~~for blocking an attack on a private network~~, comprising:

means for interconnecting ~~the private~~ a private network and a public network;

means for receiving an incoming data packet from the public network;

means for comparing a source address of the data packet against known internal addresses of the private network;

means for determining if the source address matches a known internal address; and

if there is a match, means for:

dropping the data packet;

analyzing a header of the data packet;

determining information regarding a history of the packet;

determining a real source of the data packet using the information regarding the history of the packet;

adding an IP address of the data packet to a cache of IP addresses; and

refusing to process any additional data packets received from the real source of the data packet.

32. (Currently Amended) Software embodied in a computer-readable medium, the computer-readable medium comprising code operable to:

interconnect a private network to a public network, using a routing device;

receive a request for connection from an initiator, over the public network;

request an acknowledgment from the initiator of the request, wherein the routing device requests the acknowledgment;

determine whether the acknowledgment has been received within a specific predetermined amount of time;

add an IP address of the initiator to a cache of IP addresses if the acknowledgement is not received; and

deny the request if the acknowledgment is not received within the specific predetermined amount of time.

33. (Currently Amended) Software embodied in a computer-readable medium, the computer-readable medium comprising code operable to:

receive an incoming data packet from ~~the public~~ a public network;

compare a source address of the data packet against known internal addresses of ~~the private~~ a private network, wherein a routing device that interconnects the private network and the public network compares the source address;

determine if the source address matches a known internal address; and

if there is a match:

drop the data packet;

analyze a header of the data packet;

determine information regarding a history of the packet;

determine a real source of the data packet using the information regarding the history of the packet;

add an IP address of the data packet to a cache of IP addresses; and

refuse to process any additional data packets received from the real source of the data packet.